

## REMARKS

### Allowable Subject Matter

The Examiner's indication in the current and prior Office Actions that claims 8-12 are allowed is appreciated. The Examiner's indication that claims 2 and 4 would be allowable if rewritten in independent form is also appreciated.

### Claim Rejections Under 35 U.S.C. §103

#### *Hirota + Tagawa*

Claims 1, 5-7, 13-14, and 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirota et al. (US 6,856,431) in view of Tagawa et al. (US 6,615,192).

The Examiner asserts that claim 1 is obvious under § 103 because some recitations are present in Hirota and some recitations are present in Tagawa. In particular, the Examiner asserts that Hirota teaches steps (a), (b), (c), and (f), and then relies on Tagawa for the proposition that deleting a decrypted title key, as recited in step (d) and deleting the media unique key as recited in step (e) are known. The process of decrypting a track in claim 1 is recited to comprise:

- (a) calculating a media unique key; and thereafter
- (b) decrypting a title key stored in the memory of the device with the media unique key; and thereafter
- (c) decrypting a group of frames; and thereafter
- (d) deleting the decrypted title key;
- (e) deleting the media unique key; and
- (f) repeating (a) through (e) until the entire track is completed.

Firstly, Hirota, alone or in combination with Tagawa, simply does not teach step (f). The Examiner indicates that such teachings are present at Col. 47, lines 25-27 and Col. 60, line 11 of Hirota. However, there is no such teaching of step (f) and the cyclical parsed process of decrypting a track that results from step (f) in particular, and steps (a)-(f) as a whole. To the contrary, Hirota, at Col. 47, lines 25-27 and Col. 60, line 11, appears to teach or suggest that an

*entire AOB file* is decrypted *at once* using the AOB file key. Thus, Hirota does not teach at least step (f).

Furthermore, even if, *ad arguendo*, Hirota does teach steps (a), (b), (c), and (f) and Tagawa teaches steps (d) and (e), it is kindly asserted that the invention recited in claim 1, when taken as a whole, is not taught by the combination of Hirota and Tagawa. Looking at steps (a)-(f) of claim 1, the combination does not teach such a process, when the process of decrypting a track [stored on a removable media] is viewed as a whole.

In determining the differences between the prior art and the claims, the question under 35 U.S.C. 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious. Stratoflex, Inc. v. Aeroquip Corp., 713 F.2d 1530, 218 USPQ 871 (Fed. Cir. 1983); Schenck v. Nortron Corp., 713 F.2d 782, 218 USPQ 698 (Fed. Cir. 1983). See also MPEP 2141.02. The question of obviousness necessarily turns on whether one of skill in the art would have combined the two references in the manner claimed by the invention.

There is no suggestion or teaching within either of the references that would lead one of skill in the art to arrive at the invention recited in claim 1. Just as in the Supreme Court's decision in Adams v. United States, 383 U.S. 39, 47 (1966), where a wet battery composed entirely out of prior art was held to be non-obvious because there was no previous suggestion to make the combination in the manner claimed by the patent, claim 1 is submitted to be non obvious because there is no such suggestion within Hirota and Tagawa. See also Teleflex Inc. v. KSR Int'l Co., 298 F. Supp. 2d 581 (E.D. Mich. 2003), *not citable as precedent at the Federal Circuit but cert accepted and briefs on file with the Supreme Court*.

It is not argued that deleting things, including encryption keys, is known in the art. This, however, does not mean that the invention recited in claim 1, including the process of decrypting a track [stored on a removable media] as recited in steps (a) – (f) as a whole, is obvious. Without a suggestion or teaching to combine steps (a) – (f) in the recited manner (to achieve the process of decrypting a track) from within the references, the combination necessarily relies on impermissible hindsight. While the Examiner asserts that “it must be recognized that any judgment on obviousness is in a sense necessarily based on hindsight reasoning” (Office Action at page 19-20, *citing In re McGlaughlin*), contrary to the requirements of McGlaughlin, the

arrival at the whole process recited in steps (a) – (f) is suggested by the present application and *not* by Hirota or Tagawa.

Furthermore, as mentioned earlier, contrary to teaching the iterative looping or cyclical process recited in steps (a) – (f), Hirota, at the cited portion or elsewhere, appears to teach or suggest that an entire AOB file is decrypted *at once* using the AOB file key. Thus, Hirota appears to *teach away* from the invention recited in claim 1. Therefore, Hirota and Tagawa cannot be properly combined to arrive at the invention recited by claim 1 under § 103.

To the extent that it is relevant, it is noted that the European Patent Office, in its International Preliminary Examination Report dated September 6, 2004 indicates that claim 1, identical to claim 1 of the present application, satisfies both the novelty and inventive step requirement of the PCT. This search report was submitted in an IDS on or around February 8 2005 and is of record in the current application.

Thus, it is kindly submitted, that claim 1, and the claims that depend therefrom, are not obvious under 35 USC §103. As independent claims 13 and 20 and the claims that depend therefrom were rejected upon similar reasoning, it is also submitted that those claims are in condition for allowance for similar reasons.

#### *Hirota + Tagawa + Lau*

Claims 15 and 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified system of Hirota and Tagawa as applied to claim 13 above, and further in view of Lau et al. (US 5,790,423).

Claim 15 depends from claim 13 and adds a digital signal processor (“DSP”). Claim 18 adds to that that “the secure dynamic decryption means is stored in memory of the digital signal processor, and executed by the digital signal processor,” and claim 19 adds to claim 18 that “the interface means is executed by the digital signal processor.”

The Examiner adds Lau to the combination of Hirota and Tagawa for the proposition of a digital signal processor and indicates that one of skill in the art would be motivated to make the combination in order [not] to provide real time digital signal processing. While Lau does disclose a digital signal processor, Lau does not teach use of the DSP in any encryption or decryption operation. Therefore Lau does not teach “secure dynamic decryption means is stored

in memory of the digital signal processor, and executed by the digital signal processor” as required by claim 18.

In the Examiner’s *Response to Arguments*, related to Applicant’s assertion that Lau lacks any teachings related to any encryption and/or decryption operation, including usage of its DSPs (111, and 44), the Examiner admits that “the Lau reference was merely relied upon for its teaching of a DSP.” Office Action at page 19. This substantiates the previously asserted position that there is no suggestion or teaching within the cited references to add a DSP to the system of claim 13 and to use it in the manner recited by claim 18, and that the claims were used as a roadmap to impermissibly pick and choose elements from a library of prior art. It is well accepted precedent that many novel and non obvious inventions recite combinations of individually known elements. See e.g. Adams.

In addition, one should note that the DSP recited in dependent claim 15 is in addition to the computing unit recited in independent claim 13. It is submitted that the real time digital signal processing is already present through the computing unit in independent claim 13, and that the cited motivation to combine “to provide real time digital signal processing” is therefore not adequate. To the contrary, an additional processor would increase the cost and complexity of the system and would therefore not be an obvious addition.

Therefore, it is respectfully submitted that when the invention recited in these claims is viewed as a whole, these claims cannot be properly considered obvious under § 103.

*Hirota + Tagawa + Saxena*

Claims 20-27, 28 and 38-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified system of Hirota and Tagawa as applied to claim 1 above, and further in view of Saxena et al. (US 5,805,821).

For reasons similar to those discussed with regard to claim 1, the combination of Hirota and Tagawa does not teach the limitation of claim 20 wherein “the security engine (a) decrypts one or more of the keys, (b) decrypts a portion of the encrypted content using the one or more

decrypted keys, and (c) deletes the one or more decrypted keys, and (d) repeats (a) - (c) until all portions of the content are decrypted.”

As admitted by the Examiner, the combination also does not teach “an applications programming interface for receiving the commands from the one or more user interface modules and managing the retrieval and storage of encrypted content from the secure medium.” Therefore, the Examiner has added Saxena to the combination of Hirota and Tagawa.

While Saxena does disclose usage of an API, Saxena is not related to and does not teach “a system that enables a device to decrypt a file having encrypted content on a secure medium,” as recited in the preamble to claim 20. Further, Saxena does not teach or suggest usage of its API in conjunction with a security engine for decrypting encrypted content or in conjunction with a secure system generally; there is no teaching of encryption or decryption with Saxena. Saxena relates to a video optimized media streamer user interface employing non-blocking switching to achieve isochronous data transfers. While Saxena mentions usage of an API, this is an insufficient motivation to combine.

In the *Response to Arguments* section of the latest Response, the Examiner indicates that “with respect to Applicant’s argument that the API of Saxena is not related to a system that enables a device to decrypt a file having encrypted content on a secure medium, Saxena was merely relied upon for the teaching of the use of an API...” Office action at 20. While it is true that the combination as a whole must be considered under In re Keller and In re Merck, as stated by the Examiner, it is asserted that this picking and choosing of an element without a suggestion within the references to make the combination is based upon hindsight of the impermissible variety under In re McLaughlin.

Therefore, it is kindly submitted that claims 20-27, 28, and 38-39 are in condition for allowance.

*Hirota + Tagawa + Saxena + Lau*

Claims 26, and 29-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified combination of Hirota, Tagawa, and Saxena as applied to claim 20 above, and further in view of Lau et al. (US 5,790,423).

Claims 26 and 29-32 depend from independent claim 20 and are allowable for all the reasons given above regarding independent claim 20. Claim 26 adds a digital signal processor to claim 20, and claims 29-32 recite further limitations relating the DSP. Therefore, Lau is added to the already tenuous combination of Hirota, Tagawa, and Saxena for the proposition of the DSP. Again, While Lau does disclose a digital signal processor, Lau does not teach use of the DSP in any encryption or decryption operation or the use of the DSP in conjunction with or for execution of a security engine.

It is again therefore asserted that there is no suggestion or teaching within the references that would lead one of skill in the art to combine these four references to arrive at the invention recited in claim 1. The suggestions appear to have been gleaned principally from the current application itself, contrary to the principle espoused in In re McLaughlin, cited by the Examiner. Such a combination would not be made without the benefit of the roadmap provided by the claim itself. Again, Lau does not teach use of the DSP in any encryption or decryption operation or the use of the DSP in conjunction with or for execution of a security engine.

Therefore it is kindly asserted that claims 26, and 29-32 are non obvious and are in condition for allowance.

*Hirota + Tagawa + Ansell*

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified combination of Hirota and Tagawa as applied to claim 1 above, and further in view of Ansell et al. (US 6,367,019).

In the *Response to Arguments* section of the last Office Action, the Examiner stated that “with respect to the argument that neither Hirota nor Tagawa meet the limitations of claim 3, Examiner agrees with Applicant and this rejection has been withdrawn, however, the rejection of claim 3, further in view of Ansell remains.” Office Action at page 18-19.

Referring therefore to the previous Office Action by Examiner Shewaye Gelagay, where the rejection based upon the combination of Hirota, Tagawa, and Ansell was last substantively addressed, the Examiner stated “Both references [Hirota and Tagawa] do not explicitly disclose decrypting a doubly encrypted title key stored in the media with a session key calculated while authorizing the media to produce a singly encrypted title key. Ansell, in analogous art, however,

discloses decrypting a doubly encrypted title key stored in the media with a session key calculated while authorizing the media to produce a singly encrypted title key (Col.7, line 19). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Tagawa and Dolan to include decrypting a doubly encrypted title key stored in the media with a session key calculated while authorizing the media to produce a single encrypted title key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Ansell (Col. 7, lines 20-22) in order [not] to have a secure communication between the media and the device.” Office action at page 14.

As an initial matter, it unclear what if any role the Dolan reference has in this combination, and the Examiner is kindly requested to clarify this. It will be assumed for the purposes of this Response that the Examiner meant to refer to Hirota and not Dolan. It is also assumed that the motivation put forth by the Examiner is “in order to have secure communications between the media the device,” rather than “in order not to have a secure communication between the media and the device,” as written by the Examiner.

It is respectfully asserted that claim 3 is not obvious in light of the combination of Hirota, Tagawa, and Ansell. As admitted by the Examiner, the combination of Hirota and Tagawa does not disclose “decrypting a doubly encrypted title key stored in the media with a session key calculated while authorizing the media to produce a singly encrypted title key.” The addition of Ansell to the combination does not remedy this shortcoming.

Again, Ansell, alone or in combination with Hirota and Tagawa, fails to teach all of the limitations of claim 3. Ansell teaches encrypting a media master key using a session key and sending it to the portable player 150. It is then decrypted and re-encrypted using the storage key, e.g., read-only key 504A of Ansell and sent back to player 110. See Col. 7, line 14 to line 28 of Ansell. Ansell is teaching therefore, a player to player transfer or interaction, not copying from a (removable) media to memory of the device, after decryption within the media. The teachings of Ansell are ambiguous at best about any doubly encrypted key, but if Ansell does teach a doubly encrypted key (which does not appear to be the case), it appears that such a key would be copied (from player to player) as doubly encrypted, contrary to the recitations of claim 3. Ansell,

cannot therefore teach the claim 3 recitations of “decrypting a doubly encrypted title key stored in the media with a session key calculated while authorizing the media to produce a singly encrypted title key; and copying the singly encrypted title key from the media into a memory of the device.”

Furthermore, even if Ansell teaches “decrypting a doubly encrypted title key stored in the media with a session key calculated while authorizing the media to produce a singly encrypted title key and copying the singly encrypted title key from the media into a memory of the device,” there is no suggestion within Ansell that would lead one of skill in the art to combine it with Hirota and Tagawa in order to arrive at the invention recited in claim 3. The Examiner has stated that the motivation for the combination of the three references is “in order [not] to have a secure communication between the media and the device.” This is an overly broad assertion without any specific support in the reference. There is nothing within Ansell that would suggest that secure communication requires or is enhanced by going through the trouble to remove a layer of encryption from double to single encryption before copying from media to player. To the contrary, one of skill in the art would likely be of a mindset that such a thing is not required “in order to have a secure communication between the media and the device.” One of ordinary skill in the art would likely believe that it would detract from the security.<sup>1</sup> In other words, there are many ways to skin a cat, and Ansell doesn’t disclose teach or suggest the way recited in claim 3 and any reason to combine its methodology with that of Hirota and Tagawa.

Therefore, it is kindly asserted that claim 3 is in not properly rendered obvious by the combination of Hirota, Tagawa, and Ansell, and is in condition for allowance.

*Hirota + Tagawa + Saxena + Turgeon*

Claims 33-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified combination of Hirota, Tagawa and Saxena as applied to claim 20 above, and further in view of Turgeon (US 2003-0014371).

Claim 33 is dependent and recites “the system of claim 20, further comprising:

---

<sup>1</sup> Although security is certainly important in the present invention, other driving factors e.g. authentication etc. may require the steps recited in dependent claim 3.

one or more engines for processing and transmitting audio, video or images, each engine comprising a secure application programming interface, the secure interface(s) for accessing the encrypted content and keys of the medium:

wherein each of the one or more engines for processing and transmitting audio, video or images further comprises a non-secure application programming interface for accessing unencrypted content of the medium.”

Claims 33-37 depend from independent claim 20 and are allowable for all reasons discussed with regard to that claim. Furthermore, these claims are allowable for the following additional reasons. The Examiner relies on Turgeon paragraph 12 as teaching “non-secure interface(s) for accessing the unencrypted content of the medium” of claim 33. While Turgeon does disclose accessing both encrypted and unencrypted content relating to a user’s financial data, there is no teaching of an application programming interface or “API” for doing so. An API is not a user interface, but a *programming* interface to simplify software integration. An API is also not an inherent portion of every software program, or intelligent device utilizing some form of software logic.

Furthermore, the Examiner’s contention that Turgeon is analogous art is again contested. Turgeon is not pertinent to the problem at hand, and one of skill in the art would not look to Turgeon. Turgeon is primarily concerned with financial transactions and e-commerce and has little if anything to do with playing back recorded audio, video, or other content.

The Examiner admits as much in the last action when he states that “with respect to Applicant’s argument that Turgeon does not disclose the use of a non-secure API for accessing the unencrypted content, as above Turgeon is only relied upon for the teaching of accessing unencrypted content...” Office Action at 21.

In addition, even if Turgeon is considered analogous art, one of skill in the art would not make a four (4) way combination of Hirota, Tagawa, Saxena, and Turgeon to arrive at the claimed invention without the benefit of hindsight. As discussed previously, there is no proper motivation to combine Hirota, Tagawa and Saxena in a three (3) way combination, let alone Hirota, Tagawa, Saxena, and Turgeon in a four (4) way combination. It is a very tenuous assertion that one of skill in the art would take the teachings of Turgeon’s financial transactions

and ecommerce and combine it with the other three references "in order to make the system versatile by allowing access to demos and samples" as asserted by the previous Examiner.

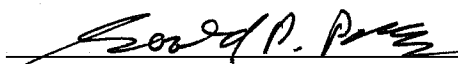
Claim 37 was previously canceled and its limitations incorporated into claim 33.

It is kindly submitted that claims 33-36 are not obvious and are in condition for allowance.

**Conclusion**

Accordingly, it is believed that this application is now in condition for allowance and an early indication of its allowance is solicited. However, if the Examiner has any further matters that need to be resolved, a telephone call to the undersigned attorney at 415-318-1163 would be appreciated.

Respectfully submitted,

  
\_\_\_\_\_  
Gerald P. Parsons  
Reg. No. 24,486

11/29/06  
\_\_\_\_\_  
Date

PARSONS HSUE & DE RUNTZ LLP  
595 Market Street, Suite 1900  
San Francisco, CA 94105  
(415) 318-1160 (main)  
(415) 318-1163 (direct)  
(415) 693-0194 (fax)